

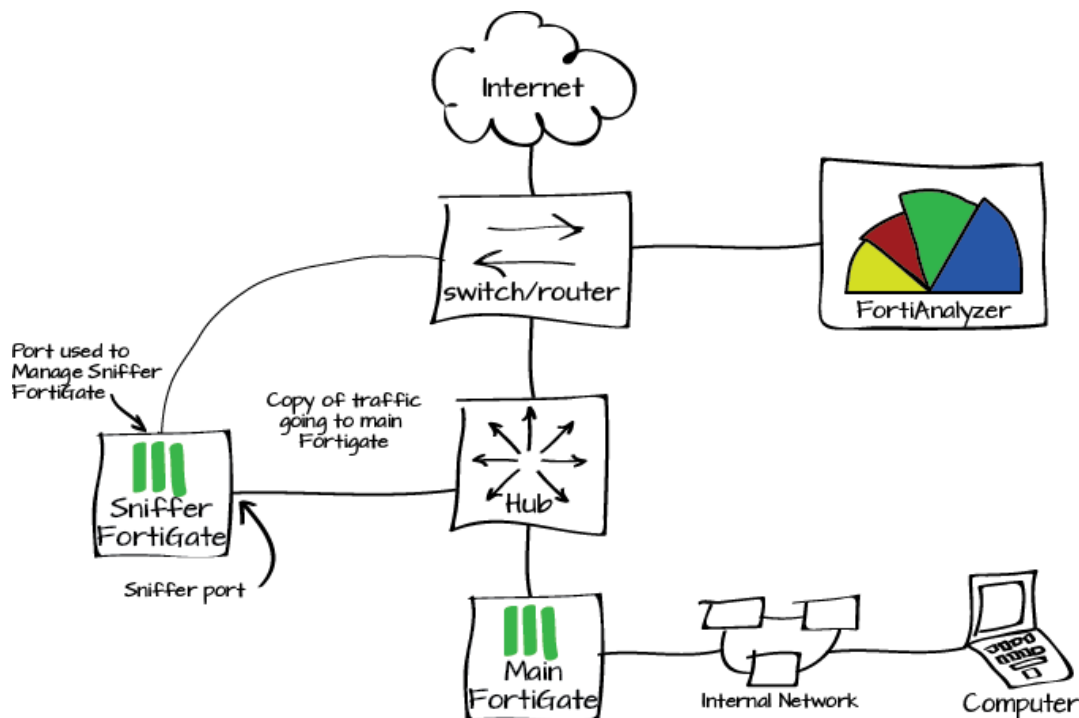
# Analyzing your network traffic using a one-armed sniffer

You can use a one-armed sniffer in coordination with a FortiAnalyzer to analyze traffic going through a main FortiGate to minimize the impact on network performance impact.

## Topology Setup

Sniffing can be done by way of port mirroring or by placing a hub between the FortiGate and the router/switch. Using a hub removes potential configuration issues with the switch.

1. Configuring the interfaces
2. Configuring the security profiles
3. Registering the sniffer device
4. Configuring logging to the FortiAnalyzer
5. Results



# Configuring the interfaces

These settings are for the FortiGate designated as the “sniffer”; in this case a FortiGate model 60D.



It is possible to use the same interface for both the mirror traffic and access to the FortiAnalyzer, but it is recommended to use one for each purpose separately.

If there is not already administratively accessible interface, consider using FortiExplorer and a USB cable.

## Configuring the Management Interface (WAN 1) on the Sniffer

Log in to the FortiGate 60D.

Go to **System > Network > Interfaces**.

Select the interface that you wish to connect to your internal network so that you can access the device remotely and allow it to connect to the FortiAnalyzer.

Verify that the configuration for the interface is completed with the information shown here. Make sure that it is on the correct subnet range.

The purpose of this interface is to manage the FortiGate and provide access to the FortiAnalyzer so it is important to make sure that the correct **Administrative Access** is chosen and that the interface is on the internal subnet.

|  |  |
|--|--|
| Name   | wan1(00:09:0F:B5:55:2A)  |
| Alias  | Management Port  |
| Link Status  | Up   |
| Type   | Physical Interface   |
| Addressing mode <input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> Dedicate to FortiAP |  |
| IP/Network Mask  | 172.20.120.69/255.255.255.0  |
| IPv6 Address   | :::0   |
| Administrative Access  | <input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP<br><input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET <input type="checkbox"/> FCT-Access <input type="checkbox"/> Auto IPsec Request |
| IPv6 Administrative Access   | <input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP<br><input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET   |
| DHCP Server  | <input type="checkbox"/> Enable  |
| Security Mode  | None   |
| Device Management  |  |
| Detect and Identify Devices  | <input type="checkbox"/>   |
| Enable Explicit Web Proxy  | <input type="checkbox"/>   |
| Listen for RADIUS Accounting Messages  | <input type="checkbox"/>   |
| Secondary IP Address   | <input type="checkbox"/>   |
| Comments   | Write a comment... 0/255   |
| Administrative Status  | <input checked="" type="radio"/> Up <input type="radio"/> Down   |
| <div>OK Cancel</div>   |  |

## Configuring the sniffer interface

Select the interface that you wish to use to collect the mirrored data traffic.

Verify that the configuration for the interface is completed with the shown information:

If the One-Arm Sniffer addressing mode is unavailable you may have to choose a different interface.

## Configuring the security profiles

Some administrators match the content of the profiles on the sniffer with those on the Main FortiGate, but this is not a requirement for the sniffer to work. The sniffer profiles will not impact your network performance so they can be as comprehensive as you want. Create profiles that will capture the information you want.



If you cannot set more than one type of Security Profile go to **System > Config > Features** and ensure that the **Multiple Security Profiles** feature is enabled.

|   |                         |
|---|-------------------------|
| Name  | wan2(00:09:0F:B5:55:2B) |
| Alias   | Sniffer Interface       |
| Link Status   | Up                      |
| Type  | Physical Interface      |
| Addressing mode<br>Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> <b>One-Arm Sniffer</b> <input checked="" type="radio"/> Dedicate to FortiAP <input type="radio"/>  |                         |
| Enable Filters <input type="checkbox"/><br><input checked="" type="checkbox"/> Include IPv6 Packets<br><input checked="" type="checkbox"/> Include Non-IP Packets   |                         |
| <b>Security Profiles</b><br><input checked="" type="checkbox"/> Enable AntiVirus Generic Flow based profile X<br><input checked="" type="checkbox"/> Enable Web Filter web-filter-flow X<br><input checked="" type="checkbox"/> Enable Application Control default X<br><input checked="" type="checkbox"/> Enable IPS all_default X                                  |                         |
| Administrative Access<br><input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP<br><input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET <input type="checkbox"/> FCT-Access <input type="checkbox"/> Auto IPsec Request |                         |
| IPv6 Administrative Access<br><input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP<br><input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET  |                         |
| Enable Explicit Web Proxy <input type="checkbox"/>  |                         |
| Listen for RADIUS Accounting Messages <input type="checkbox"/>  |                         |
| Secondary IP Address <input type="checkbox"/>   |                         |
| Comments<br>Write a comment... 0/255  |                         |
| Administrative Status<br><input checked="" type="radio"/> Up <input type="radio"/> Down   |                         |
| <div>OK Cancel</div>  |                         |

### Multiple Security Profiles ?

ON



# AntiVirus Profile (Flow-based)

Go to **Security Profiles > AntiVirus > Profiles**.

Apply the same settings to the profile on the sniffer device as on the primary FortiGate.



The one-armed sniffer mode will only allow flow-based profiles to be used.

Configure the following in the CLI, in addition to the web-based configuration:

Name

Generic Flow based profile

Comments

Write a comment... 0/255

Inspection Mode

☐ Proxy ☒ Flow-based

☒ Block Connections to Botnet Servers

| Protocol             | Virus Scan and Removal              |
|----------------------|-------------------------------------|
| <b>Web</b>           |                                     |
| HTTP                 | <input checked="" type="checkbox"/> |
| <b>Email</b>         |                                     |
| SMTP                 | <input checked="" type="checkbox"/> |
| POP3                 | <input checked="" type="checkbox"/> |
| IMAP                 | <input checked="" type="checkbox"/> |
| <b>File Transfer</b> |                                     |
| FTP                  | <input checked="" type="checkbox"/> |
| SMB                  | <input checked="" type="checkbox"/> |

Apply

```
config antivirus settings
  set default-db normal
end

config antivirus profile
  edit AV-flow
    set extended-utm-log enable
    config smb
      set options scan
    end
    set av-virus-log enable
    set av-block-log enable
  end
end
```

# Application Control Sensor

Go to **Security Profiles > Application Control > Application Sensors**.

Apply the same settings to the profile on the sniffer device as on the primary FortiGate.

Add the these CLI settings in addition to the web-based configuration:

Name

default

Comments

monitor all applications

24/255

☒ Allow and Log DNS Traffic

Create New

Copy

Import

Delete

Reset

| Category       | Popularity | Technolo... | Risk | Action  | Application                            |
|----------------|------------|-------------|------|---------|--|
| All + Uncommon | ☆☆☆☆☆      | All         | All  | Monitor | 012mail,0zz0,1and1 ... [Show all 3118] |
|                |            |             |      | Monitor | All Other Known Applications           |
|                |            |             |      | Monitor | All Other Unknown Applications         |

Apply

```
config application list
  edit "default"
    set extended-utm-log enable
    set other-application-log enable
    set log enable
    set unknown-application-log enable
  end
```

## Webfilter Profile (Flow-based)

Go to **Security Profiles > Webfilter > Profiles**.

Apply the same settings to the profile on the sniffer device as on the primary FortiGate.

Name

Comments  29/255

Inspection Mode ☐ Proxy ☒ Flow-based ☐ DNS

☒ FortiGuard Categories

Show All X

Local Categories

Potentially Liable

Adult/Mature Content

Bandwidth Consuming

Security Risk

General Interest - Personal

General Interest - Business

Unrated

☐ Enable Safe Search

☒ Scan Encrypted Connections

☐ Enable Web Site Filter

☐ Web Content Filter

☐ Allow Websites When a Rating Error Occurs

☐ Rate URLs by Domain and IP Address

**Apply**

Configure the following settings in the CLI, in addition to the web based configuration:

```
config webfilter profile
  edit web-filter-flow
    set extended-utm-log enable
    set options https-url-scan
  end
```

IPS sensor

Go to **Security Profiles > Webfilter > Profiles**.

Apply the same settings to the sensor on the sniffer device as on the primary FortiGate.

Registering the Sniffer device

Log in to the FortiAnalyzer.

Go to the **Device Manager** tab.

Select **Add Device** from the drop down menu.

In the **Login** screen of the **Add Device** wizard fill in the fields with the information shown here.

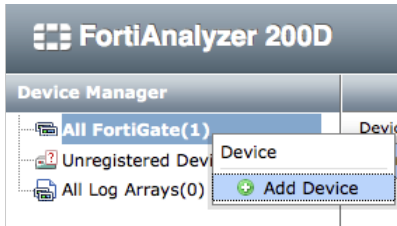
Select **Next**.

Name: all\_default

Comments: all predefined signatures with default setting 46/255

| Severity | Targ... | OS  | Action  | Packet Logging | Matched Signatures  |
|----------|---------|-----|---------|----------------|---|
| All      | All     | All | Monitor | Enable         | 2Wire.Wireless.Router.XSRF.Password.Reset<br>3Com.3CDaemon.FTP.Server.Buffer.Overflow<br>...<br>[Show all 6593] |

Apply



Add Device

Login

Please choose one of the following methods for adding a device or vdom.

**Add Model Device**

Device will be added using the chosen model type and other explicitly entered information.

Please enter the following information:

|            |               |
|------------|---------------|
| IP Address | 172.20.120.69 |
| User Name  | admin         |
| Password   |               |

Next > Cancel

In the **Add Device** screen of the **Add Device** wizard fill in the fields with the information shown here.

If there is no more information to enter, select **Next**.

Select the sideways triangle next to **Other Device Information** to expand the window for more field options.

Select **Next**.

## Add Device

Please input the following information to complete addition of the device:

|                                   |  |                                 |
|-----------------------------------|--|---------------------------------|
| Name                              | <input type="text" value="One-Arm_Sniffer-1"/>   |                                 |
| Description                       | <input type="text" value="Sniffer_for_FG100D"/>  |                                 |
| Device Type                       | <input type="text" value="FortiGate"/>   |                                 |
| Device Model                      | <input type="text" value="FortiGate-60D"/>   |                                 |
| Firmware Version                  | <input type="text" value="5.0"/>   | <input type="text" value="GA"/> |
| SN                                | <input type="text" value="FGT60D4613001043"/>  |                                 |
| Enable Interface Mode             | <input checked="" type="checkbox"/>  |                                 |
| Disk Log Quota (min. 100MB)       | <input type="text" value="1000"/>  | MB (Total 783,298 MB Available) |
| When Allocated Disk Space is Full | <input checked="" type="radio"/> Overwrite Oldest Logs <input type="radio"/> Stop Logging  |                                 |
| Log Storage                       | <input checked="" type="radio"/> Standalone Logs <input type="radio"/> Log Array   |                                 |
| Device Permissions                | <input checked="" type="checkbox"/> Logs <input checked="" type="checkbox"/> DLP Archive <input checked="" type="checkbox"/> Quarantine <input checked="" type="checkbox"/> IPS Packet Log |                                 |
| ▶ Other Device Information        |  |                                 |

Device Permissions ☒ Logs ☒ DLP Archive ☒ Quarantine ☒ IPS Packet Log

### ▼ Other Device Information

|                      |  |
|----------------------|--|
| Company/Organization | <input type="text" value="Daily Planet"/>  |
| Contact              | <input type="text" value="P. White"/>      |
| City                 | <input type="text" value="Metropolis"/>    |
| Province/State       | <input type="text" value="DC"/>            |
| Country              | <input type="text" value="United States"/> |



A window showing successful registration should appear.

Select **Next** to proceed.

The final window of the wizard provides a summary of the configuration.

### Add Device

|            |  |
|------------|--|
| Name       | One-Arm_Sniffer-1  |
| IP Address | 172.20.120.69  |
| Status     | <div><div><div>✔</div>Device created successfully</div><div><div>✔</div>Creating device database</div><div><div>✔</div>Retrieving high availability status</div><div><div>✔</div>Initializing configuration database</div><div><div>✔</div>Updating group membership</div></div> |

### Model Device Added Successfully

The following device has been added to the system:

|                      |                             |
|----------------------|-----------------------------|
| Name                 | One-Arm_Sniffer-1           |
| Description          | Sniffer_for_FG100D          |
| Hostname             | N/A                         |
| IP Address           | 172.20.120.69               |
| Admin User           | admin                       |
| Device Model         | FortiGate-60D               |
| Firmware Version     | 5.0 GA                      |
| SN                   | FGT60D4613001043            |
| Disk Allocation      | 1000 MB                     |
| Company/Organization | Daily Planet                |
| Contact              | P. White                    |
| City                 | Metropolis DC United States |

# Configure logging to the FortiAnalyzer

Go to **Log & Filter > Log Config > Log Settings.**

Configure the settings as shown here.

Be sure to test the connectivity before proceeding.

**Logging and Archiving**

☒ Send Logs to FortiAnalyzer/FortiManager

IP Address:

Upload Option

☒ Realtime

☐ Encrypt Log Transmission

☐ Send Logs to FortiCloud

Account:

☒ Event Logging

☒ Enable All

☒ WiFi activity event

☒ System activity event

☒ User activity event

☒ Router activity event

☒ VPN activity event

☒ Explicit web proxy event

**Local Traffic Logging**

☒ Log Allowed Traffic

☒ Log Local Out Traffic

☒ Log Denied Traffic

**GUI Preferences**

Display Logs From

☒ Resolve Hostnames (Using reverse DNS lookup)

☒ Resolve Unknown Applications (Using remote application database)

## Results

### Creating some logs

On a computer behind the primary FortiGate, download some test files from the Eicar website at:

<http://www.eicar.org/85-0-Download.html>

Visit some websites that should be blocked by the policy, for example:

[www.gambling.com](http://www.gambling.com)

# Seeing the results on the FortiAnalyzer

Log in to the FortiAnalyzer

Go to the **Log View** tab.

In the left-hand column, expand the tree for the sniffer device.

Go to **Security > Intrusion Prevention**.

You will see a listing of the items that are considered relevant.

In this case the one for the test file shows the **Attack Name** as Eicar.Virus.Test.File

FortiAnalyzer 200D

Device ManagerLog ViewDrill DownEvent ManagementReportsSystem Settings

Log View

srcip=172.16.86.11 vd=vdom2

Any time

| # | Date/Time   | Severity | Source/Device  | Destination IP | Status   |
|---|-------------|----------|----------------|----------------|----------|
| 1 | 02-27 11:34 | low      | 74.217.253.60  | 192.168.10.103 | detected |
| 2 | 02-27 11:34 | low      | 74.217.253.60  | 192.168.10.103 | detected |
| 3 | 02-27 11:34 | low      | 173.194.43.77  | 192.168.10.103 | detected |
| 4 | 02-27 11:03 | info     | 188.40.238.250 | 192.168.10.103 | detected |

50Items per page<< first< prev1next>> last>>Go to

Log DetailsArchive

|                  |                                      |                     |
|------------------|--------------------------------------|---------------------|
| Attack ID        | 29844                                | Attack Name         |
| Count            | 1                                    | Date/Time           |
| Destination IP   | 192.168.10.103                       | Destination Name    |
| Destination Port | 54133                                | Device ID           |
| Device Time      | 2014-02-27 11:03:41                  | Event Type          |
| Identity Index   | 0                                    | Incident Serial No. |
| Level            | alert                                | Log ID              |
| Message          | file_transfer: Eicar.Virus.Test.File | Policy ID           |
| Protocol         | 6                                    | Reference           |
| Sensor           | all_default                          | Sequence No.        |
| Service          | 54133/tcp                            | Severity            |
| Source Interface | wan2                                 | Source Port         |
| Source/Device    | 188.40.238.250                       | Status              |
| Sub Type         | ips                                  | Time Stamp          |
| Type             | utm                                  | Virtual Domain      |

Select the **Log View** Tab.

In the left-hand column, expand the tree for the sniffer device.

Select **Traffic**.

Use the column filters to focus in on the target traffic. In this case we are looking for traffic with:

- Source IP address = 192.168.10.100
- Destination IP address = 190.93.240.30
- Service = HTTP

FortiAnalyzer 200D

Device ManagerLog ViewDrill DownEvent ManagementReportsSystem Settings

Log View

srcip=172.16.86.11 and service=HTTP

Any time

| # | Date/Time | Policy ID | Threat | Status | Source/Device  | Destination IP | Service |
|---|-----------|-----------|--------|--------|----------------|----------------|---------|
| 1 | 14:58:36  | 1         |        | accept | 192.168.10.100 | 190.93.240.30  | HTTP    |
| 2 | 14:58:34  | 1         |        | accept | 192.168.10.100 | 190.93.240.30  | HTTP    |
| 3 | 14:58:32  | 1         |        | accept | 192.168.10.100 | 190.93.240.30  | HTTP    |
| 4 | 14:56:27  | 1         |        | accept | 192.168.10.100 | 190.93.240.30  | HTTP    |

50Items per page<< first< prev1next>> last>>Go to page 1 of 1

Log Details

|                  |                      |                       |                     |
|------------------|----------------------|-----------------------|---------------------|
| Application      | HTTP.BROWSER_Firefox | Application Category  | Web.Others          |
| Application ID   | 34050                | Date/Time             | 14:58:36            |
| Destination IP   | 190.93.240.30        | Destination Interface | N/A                 |
| Destination Port | 80                   | Device ID             | FGT6004613001043    |
| Device Time      | 2014-03-31 14:58:35  | Duration              | 0                   |
| Level            | notice               | Log ID                | 13                  |
| Policy ID        | 1                    | Protocol              | 6                   |
| Sent/Received    | 0 / 597 B            | Sequence No.          | 7974                |
| Service          | HTTP                 | Source Country        | Reserved            |
| Source Interface | wan2                 | Source Port           | 12626               |
| Source/Device    | 192.168.10.100       | Status                | accept              |
| Sub Type         | forward              | Time Stamp            | 2014-03-31 14:58:36 |
| Tran Display     | snat                 | Type                  | traffic             |
| Virtual Domain   | root                 |                       |                     |



The destination address was determined by pinging gambling.com and looking at the resolved address.